

Route Insight Manager Appliance Quick Start

September 2009

This document describes how to install the Route Insight Manager Appliance, Version 8.0.

Contents

| | |
|---|----|
| Overview | 3 |
| About the Route Insight Manager Appliance | 3 |
| Front and Back Panel Overview and Features | 3 |
| Route Insight Manager Platform Hardware Specifications | 4 |
| Route Insight Manager FRUs | 5 |
| Installation Environment Setup | 6 |
| Rack Requirements and Specifications for a Route Insight Manager Appliance | 6 |
| Environmental Requirements for a Route Insight Manager Appliance | 7 |
| Power Requirements for a Route Insight Manager Appliance | 8 |
| Safety | 9 |
| General Safety Guidelines and Warnings for Route Insight Manager Appliances | 9 |
| Fire Safety Requirements for the Route Insight Manager Appliance | 10 |
| Route Insight Manager Appliance Agency Approvals | 11 |
| Installation | 12 |
| Unpacking the Appliance | 12 |
| Attaching Mounting Brackets | 14 |
| Installing the Appliance in a Rack | 14 |
| Connecting a Console to the Appliance | 15 |
| Configuring Basic Settings | 15 |
| Boot Sequence | 16 |
| Show Configuration | 17 |
| Configure Ethernet | 17 |
| Configure Network | 18 |

| | |
|--|----|
| Configure DNS | 19 |
| Configure Passwords Menu | 19 |
| Configure Technical Support Access | 21 |
| Diagnostics Menu | 22 |
| Reboot | 23 |
| Shutdown | 24 |
| List of Technical Publications | 24 |
| Revision History | 31 |

Overview

The Route Insight Manager Appliance Quick Start Guide contains the following topics:

- About the Route Insight Manager Appliance on page 3
- Front and Back Panel Overview and Features on page 3
- Route Insight Manager Platform Hardware Specifications on page 4

About the Route Insight Manager Appliance

Route Insight Manager is a route analytics tool that provides insight into real-time routing topology and monitors vital service parameters such as network churn and prefix flaps, alerting you to potential problems and allowing before and after comparisons and event analysis.

Route Insight Manager appliances are easy to deploy. The appliances physically connect to the network directly to one of the routers or through a switch or hub. The appliances establish communication with several routers in the network through the routing protocol over the single physical connection. Link-state routers send periodic update messages that communicate network information to each other, and to the appliance.

You can monitor and record network events in different parts of the network with multiple route recorder units. The distributed recorders collect routing data locally, from the area where they are installed, through generic route encapsulation (GRE) tunnels, or both. A centralized Management Console retrieves the data from each recorder. For a description of recorder configuration, see the “Configuration and Management” chapter in the *Route Insight Manager Administrator’s Guide*.

Front and Back Panel Overview and Features

The Route Insight Manager appliance is shown in Figure 1 on page 3 and has a 2U rack-mountable chassis with optional redundant AC and DC power supplies, a 2U hot-swappable mirrored RAID1 array, 12 GB of memory, and a Gigabit Ethernet controller.

Figure 1: Front Panel View



The following tables describe the features of the front panel for the Route Insight Manager appliance. The chassis, hard drive, and LAN LEDs are described in Table 1 on page 4.

Table 1: Appliance Front Panel LEDs

| Description |
|---|
| <p>Chassis LEDs</p> <ul style="list-style-type: none"> ■ Power (green) - When lit, indicates that the appliance is powered on ■ Hard disk (yellow) - When lit, indicates the hard disk is in use (writing or reading data) ■ Hardware (red) - When lit, indicates that a fan, power supply, or temperature alarm has occurred <p>LAN LEDs</p> <ul style="list-style-type: none"> ■ Left LED (green) - When lit, indicates that the link is active ■ Right LED - Indicates the link speed: <ul style="list-style-type: none"> ■ off - 10 Mbps ■ green - 100 Mbps ■ yellow - 1 Gbps <p>Hard drive tray LEDs</p> <ul style="list-style-type: none"> ■ Left (green) - For disk activity ■ Right (red) - For disk failure |

Route Insight Manager Platform Hardware Specifications

The appliance has the following ports:

- Serial Console—One RJ45 serial port.
- Network ports—Four RJ45 10/100/1000 Ethernet ports.
- USB interface for Flash drive.

The appliance chassis front panel has LEDs as described in Table 2 on page 4.

Table 2: Route Insight Manager Appliance Chassis LEDs

| LED | Meaning |
|------------|--|
| Power | When lit, indicates power is applied to the appliance. |
| HW Warning | When lit, indicates a hardware problem on the appliance. |

Route Insight Manager FRUs

The following sections describe the field replaceable units (FRUs) in the Route Insight Manager appliance chassis.

- Hard Drive on page 5
- Power Supply on page 5
- Fans on page 6

Hard Drive

The Route Insight Manager appliance ships with hot-swappable hard disks to offer component redundancy. The appliance has a RAID10 configuration of six 500 GB SAS drives (5001) or four 1TB SAS drives (5002). Redundant disks maintain a copy of the software image and configuration information as it is on working drives. If the working drive fails, the redundant drive immediately assumes responsibility for Route Insight Manager operations. You can hot-swap the disk if any one of the disk drives fails. The drives are externally accessible.

Redundant array of independent disk (RAID) is an organization of multiple disks to enhance fault tolerance and performance. It is used in the servers for data storage and to replicate data among multiple hard disk drives. There are different RAID levels designed to increase data reliability and increased I/O performance. In RAID10, drives are striped for performance, and all striped drives are duplicated for fault tolerance.

The key concepts in RAID are:

- Mirroring - copy data to more than one disk
- Striping - split data across more than one disk
- Error correction - redundant data storage to detect and resolve problems

The hard drive LEDs are described in Table 3 on page 5.

Table 3: Hard Drive LEDs

| LED | Meaning |
|-------|-------------------------------------|
| LED 1 | When lit, indicates drive activity. |
| LED 2 | When lit, indicates drive failure. |

Power Supply

The appliance has a dual hot swap redundant 560W AC power supply module, and can support additional redundant power supply modules. If one power supply fails, an optional second power supply can assume responsibility for the entire power load. The appliances also have a hot swap dual redundant 560W DC power supply

option if you need DC power. You can have both AC and DC power supplies in the same chassis.

Fans

The Route Insight Manager platform appliance contains three hot-swappable redundant cooling fans.

Installation Environment Setup

This section contains the following topics:

- Rack Requirements and Specifications for a Route Insight Manager Appliance on page 6
- Environmental Requirements for a Route Insight Manager Appliance on page 7
- Power Requirements for a Route Insight Manager Appliance on page 8

Rack Requirements and Specifications for a Route Insight Manager Appliance

The Route Insight Manager appliance can be installed in many types of racks, including four-post Telco racks and open-frame racks. Table 4 on page 6 lists the rack requirements.

Table 4: Route Insight Manager 500 Rack Requirements

| Rack Requirement | Guidelines |
|-------------------------|---|
| Rack type | Use a front mount rack, four-post rack (Telco), or a center-mount rack. |
| Rack size and strength | <ul style="list-style-type: none"> ■ Ensure that the rack complies with one of these standards: <ul style="list-style-type: none"> ■ A 19-in. rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronics Industry Association (http://www.eia.org). ■ A 600-mm rack as defined in the four-part Equipment Engineering (EE); European telecommunications standard for equipment practice (document numbers ETS 300 119-1 through 119-4) published by the European Telecommunications Standards Institute (http://www.etsi.org). The horizontal spacing between the rails in a rack that complies with this standard is wider than the appliance's mounting brackets, which measure 19 in. (48.2 cm) from outer edge to outer edge. Use approved wing devices to narrow the opening between the rails as required. ■ Ensure that the spacing of rails and adjacent racks allow for the proper clearance around the appliance and rack. |

Table 4: Route Insight Manager 500 Rack Requirements (continued)

| Rack Requirement | Guidelines |
|---------------------------------------|--|
| Rack connection to building structure | <ul style="list-style-type: none"> ■ Secure the rack to the building structure. ■ If earthquakes are a possibility in your geographical area, secure the rack to the floor. ■ Secure the rack to the ceiling brackets as well as wall or floor brackets if maximum stability is required. |

One pair of mounting brackets is supplied with the appliance. The holes in the mounting brackets are spaced at 1 U (1.75 in. or 4.445 cm), so the appliance can be mounted in any rack that provides holes spaced at that distance.

The outer edges of the mounting brackets extend the width of the chassis to 19 in. (48.2 cm), and the front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting brackets. The spacing of rails and adjacent racks must also allow for the clearances around the appliance and rack.

Environmental Requirements for a Route Insight Manager Appliance

The appliance must be installed in a rack or cabinet housed in a dry, clean, well-ventilated, and temperature-controlled environment.

Ensure that these environmental guidelines are followed:

- The site must be as dust-free as possible, because dust can clog air intake vents and filters, reducing the efficiency of the appliance cooling system.
- Maintain ambient airflow for normal appliance operation. If the airflow is blocked or restricted, or if the intake air is too warm, the appliance might overheat. Table 5 on page 7 provides the required environmental conditions for normal appliance operation.

Table 5: Environmental Requirements for Appliance Operation

| Description | Tolerance |
|-------------------|--|
| Altitude | No performance degradation to 10,000 feet (3048 meters) |
| Relative Humidity | Normal operation ensured in relative humidity range of 8% to 90%, non-condensing |
| Temperature | Normal operation ensured in temperature range of 41° F to 104° F (5° C to 40° C) |

The operational environment must also be able to withstand the heat and noise generation shown in Table 6 on page 8.

Table 6: Appliance Heat and Noise Dissipation

| Description | Output |
|--|--|
| Thermal dissipation | With a single power supply: <ul style="list-style-type: none"> ■ 323 BTU/hr (94.67 W) typical ■ 413 BTU/hr (121 W) maximum With dual power supplies: <ul style="list-style-type: none"> ■ 413 BTU/hr (121 W) typical ■ 499 BTU/hr (146.26) maximum |
| Acoustic noise from approximately 3 feet | <ul style="list-style-type: none"> ■ Front/rear with 1 power supply xx/xx DB. ■ Front/rear with 2 power supplies xx/xx DB. |

Table 7 on page 8 lists the environmental requirements for storing the appliance while non-operational.

Table 7: Environmental Requirements for Appliance Storage

| Description | Tolerance |
|-------------------|---|
| Altitude | The appliance can be stored safely up to an altitude of 40,000 feet (12,192 meters) |
| Relative Humidity | The appliance can be stored safely in relative humidity range of 5% to 95%, non-condensing |
| Temperature | The appliance can be stored safely in temperature range of -40° F to 158° F (-40° C to 70° C) |

Power Requirements for a Route Insight Manager Appliance

A Route Insight Manager appliance can be powered by either an AC or DC electrical supply, depending on the power modules that shipped in your appliance. Table 8 on page 8 shows the electrical power requirements for a Route Insight Manager appliance with AC power modules.

Table 8: Power Requirements for Route Insight Manager Appliances with AC Power Modules

| Item | Requirement |
|-------------------------|--|
| AC input voltage | 90 to 264 VAC |
| AC input line frequency | 50 to 60 Hz |
| AC current rating | 25 A (low appliance) 60 A (mid appliance) |

Table 8: Power Requirements for Route Insight Manager Appliances with AC Power Modules (continued)

| Item | Requirement |
|----------------------|-----------------------|
| Maximum output power | 400 W (low appliance) |
| | 700 W (mid appliance) |

Table 9 on page 9 shows the electrical power requirements for a Route Insight Manager appliance with DC power modules.

Table 9: Power Requirements for Appliances with DC Power Modules

| Item | Requirement |
|-------------------------|-------------|
| DC input voltage | -48 VDC |
| DC input current rating | 60 A |
| Maximum output power | 710 W |

Safety

This section contains the following topics:

- General Safety Guidelines and Warnings for Route Insight Manager Appliances on page 9
- Fire Safety Requirements for the Route Insight Manager Appliance on page 10
- Route Insight Manager Appliance Agency Approvals on page 11

General Safety Guidelines and Warnings for Route Insight Manager Appliances

The following guidelines help ensure your safety and protect the appliance from damage. The list of guidelines might not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

- Perform only the procedures explicitly described in the hardware documentation for this product. Make sure that only authorized service personnel perform other system services.
- Keep the area around the chassis clear and free from dust before, during, and after installation.
- Keep tools away from areas where people could trip over them while walking.
- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the chassis.
- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.

- Do not perform any actions that create a potential hazard to people or make the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.
- Operate the appliance only when it is properly grounded.
- Ensure that the separate protective earthing terminal provided on this product is permanently connected to earth.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet-metal parts unless instructions are provided in the hardware documentation for this product. Such an action could cause severe electrical shock.
- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.
- Avoid spilling liquid onto the appliance. Such an action could cause electrical shock or damage the appliance.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.
- Always ensure that all modules, power supplies, and blanks are fully inserted and that the installation screws are fully tightened.

Fire Safety Requirements for the Route Insight Manager Appliance

In the event of a fire emergency involving switches and other network equipment, the safety of people is the primary concern. You should establish procedures for protecting people in the event of a fire emergency, provide safety training, and properly provision fire control equipment and fire extinguishers.

In addition, you should establish procedures to protect your equipment in the event of a fire emergency. Juniper Networks products should be installed in an environment suitable for electronic equipment. We recommend that fire suppression equipment be available in the event of a fire in the vicinity of the equipment, and that all local fire, safety, and electrical codes and ordinances be observed when installing and operating your equipment.

Fire Suppression

In the event of an electrical hazard or an electrical fire, you should first turn power off to the equipment at the source. Then use a Type C fire extinguisher, which uses noncorrosive fire retardants, to extinguish the fire.

Fire Suppression Equipment

Type C fire extinguishers, which use noncorrosive fire retardants such as carbon dioxide and Halotron™, are most effective for suppressing electrical fires. Type C fire

extinguishers displace oxygen from the point of combustion to eliminate the fire. For extinguishing fire on or around equipment that draws air from the environment for cooling, you should use this type of inert oxygen displacement extinguisher instead of an extinguisher that leaves residues on equipment.

Do not use multipurpose Type ABC chemical fire extinguishers (dry chemical fire extinguishers). The primary ingredient in these fire extinguishers is monoammonium phosphate, which is very sticky and difficult to clean. In addition, in the presence of minute amounts of moisture, monoammonium phosphate can become highly corrosive and corrodes most metals.

Any equipment in a room in which a chemical fire extinguisher has been discharged is subject to premature failure and unreliable operation. The equipment is considered to be irreparably damaged.



NOTE: To keep warranties effective, do not use a dry chemical fire extinguisher to control a fire at or near a Juniper Networks appliance. If a dry chemical fire extinguisher is used, the unit is no longer eligible for coverage under a service agreement.

We recommend that you dispose of any irreparably damaged equipment in an environmentally responsible manner.

Route Insight Manager Appliance Agency Approvals

The appliance complies with the following standards:

- Safety
 - CSA 60950-1 (2003), Safety of Information Technology Equipment
 - UL 60950-1 (2003), Safety of Information Technology Equipment
 - EN 60950-1 (2001), Safety of Information Technology Equipment
 - IEC 60950-1 (2001), Safety of Information Technology Equipment (with country deviations)
 - EN 60825-1 + A1 + A2 (1994) Safety of Laser Products — Part 1: Equipment Classification
 - EN 60825-2 (2000), Safety of laser products – Part 2: Safety of Optical Fiber Communications Systems
- EMC
 - EN 300 386 V1.3.3 (2005), Telecom Network Equipment — EMC Requirements
- EMI
 - FCC Part 15 Class A (2007), USA Radiated Emissions
 - EM 55022 Class A (2006), European Radiated Emissions

- VCCI Class A (2007), Japanese Radiated Emissions
- Immunity
 - EN 55024 + A1 + A2 (1998) Information Technology Equipment Immunity Characteristics
 - EN-61000-3-2 (2006) Power Line Harmonics
 - EN-61000-3-3 + A1 + A2 + A3 (1995) Power Line Voltage Fluctuations
 - EN-61000-4-2 + A1 + A2 (1995) Electrostatic Discharge
 - EN-61000-4-3 + A1 + A2 (2002) Radiated Immunity
 - EN-61000-4-4 (2004) Electrical Fast Transients
 - EN-61000-4-5 (2006) Surge
 - EN-61000-4-6 (2007) Immunity to Conducted Disturbances
 - EN-61000-4-11 (2004), Voltage Dips and Sags

Installation

This section contains the procedure to install and initially set up your Route Insight Manager appliance. The following sequence of steps are included:

- Unpacking the Appliance on page 12
- Attaching Mounting Brackets on page 14
- Installing the Appliance in a Rack on page 14
- Connecting a Console to the Appliance on page 15
- Configuring Basic Settings on page 15
- Boot Sequence on page 16
- Show Configuration on page 17
- Configure Ethernet on page 17
- Configure Network on page 18
- Configure DNS on page 19
- Configure Passwords Menu on page 19
- Configure Technical Support Access on page 21
- Diagnostics Menu on page 22
- Reboot on page 23
- Shutdown on page 24

Unpacking the Appliance

The Route Insight Manager appliance is shipped in a cardboard carton and is secured with foam packing material. The carton also contains an accessory box.



CAUTION: The appliance is maximally protected inside the shipping carton. Do not unpack it until you are ready to begin installation.



WARNING: The appliance weighs over 26 lbs (approximately 12 Kg). Use correct lifting technique when moving the appliance.

To unpack the appliance:

1. Move the shipping carton to a staging area as close to the installation site as possible, but where you have enough room to remove the system components.
2. Position the carton so that the arrows are pointing up.
3. Open the top flaps on the shipping carton.
4. Remove the accessory box and verify the contents against the parts inventory on the label attached to the carton.
5. Pull out the packing material holding the appliance in place.
6. Read “General Safety Guidelines and Warnings” with particular attention to “Chassis Lifting Guidelines.”
7. Remove the appliance from the carton.
8. Verify the chassis components received against the packing list included with the switch. Table 10 on page 13 provides an inventory of parts provided with the appliance.
9. Save the shipping carton and packing materials in case you need to move or ship the appliance later.

Table 10: Inventory of Components Provided with the Appliance

| Component | Quantity |
|---|----------|
| Appliance chassis | 1 |
| Fan tray (preinstalled) | 3 |
| Power supply (preinstalled) | 1 or 2 |
| Hard drive (preinstalled) | 4 or 6 |
| Power cord retainer clip | 1 |
| Mounting brackets | 2 |
| Mounting screws | 8 |
| RJ-45 cable and RJ-45 to DB-9 serial port adapter | 1 |

Attaching Mounting Brackets

To install your appliance in a rack, you must attach mounting brackets to it.

Your appliance is shipped with one pair of mounting brackets. The holes in the mounting brackets are spaced at 1 U (1.75 in. or 4.445 cm), so the appliance can be mounted in any rack that provides holes spaced at that distance.

The outer edges of the mounting brackets extend the width of the chassis to 19 in. (48.2 cm). The spacing of rails and adjacent racks must also allow for the clearances around the appliance and rack.

The chassis and brackets are designed to allow front, middle, or rear mounting.

You need a Phillips (+) screwdriver, number 2 to mount the brackets.

To attach each mounting bracket to the appliance:

1. Place the appliance on a flat, stable surface.
2. Align the mounting brackets along the front, rear, or center of a side panel of the appliance chassis, depending on how you want to mount the appliance in a rack. For example, if you want to center-mount the appliance, align the mounting brackets along the center of the side panel.
3. Align the bottom hole in the mounting bracket with a hole on the side panel on the appliance chassis.
4. Insert one mounting screw (provided in the accessory box shipped with the appliance) into each of the two aligned holes. Use a Phillips (+) screwdriver, number 2 to tighten the screw to the chassis. Ensure that the other holes in the mounting bracket are aligned with the corresponding holes in the side panel.
5. Insert screws into the other holes in the mounting bracket aligned with the holes in the side panel and tighten the screws to the chassis using a Phillips (+) screwdriver, number 2.

Installing the Appliance in a Rack

Ensure these tasks are completed before installing the appliance in a rack:

- Unpack the appliance, as described in “Unpacking an Appliance” on page 3.
- Remove the appliance from the shipping container and place it on a flat surface.
- Attach the mounting brackets to the chassis, as described in “Attaching Mounting Brackets” on page 3

To install the appliance in a rack:

1. Attach the chassis to the rack. We recommend that two people perform this step: one person to hold the chassis in place while the other inserts the screws.



WARNING: Use correct lifting technique when moving the appliance.

- Align the holes in the mounting bracket with the holes in the rack rails.
 - Insert the screws in each of the holes and tighten them with a Phillips (+) screwdriver, number 2.
2. Plug the Ethernet cable into the network port marked ETH0 on the front panel.
 3. Plug the null modem serial cable into the console port.

A null modem cable was shipped with the appliance. If you do not have that cable, use any other null modem serial cable.

The basic hardware installation is now complete. The next step is to connect the appliance to a console.

Connecting a Console to the Appliance

To connect to the Route Insight Manager appliance for the first time, you must attach it to a console terminal running an emulation utility such as HyperTerminal.

To connect the console:

1. Configure a console terminal or terminal emulation utility to use the following serial connection parameters:
 - 9600 bits per second
 - 8-bit no parity (8N1)
 - 1 stop bit
 - No flow control
2. Connect the terminal or laptop to the null modem serial cable plugged into the appliance console port.

The next step is to power on and perform initial setup.

Configuring Basic Settings



CAUTION: By default, the appliance requires a static IP address. If you use Dynamic Host Configuration Protocol (DHCP) (not recommended) to acquire an IP address, serious problems can occur when the IP address changes. For example, you will be unable to view database information on the web-based user interface.

Perform these steps to configure the basic settings of the appliance:

1. Power on the appliance by pressing the power button on the front panel. The power LED light illuminates when the power is on.

2. Set the IP address using the serial console interface.
3. Connect Port 1 to the LAN using the CAT5 10/100/1000 Base-TX cable supplied with the appliance.

Table 11: Serial Port Settings

| Feature | Setting |
|-----------------------|----------|
| Baud rate | 9600 bps |
| Bits | 8 |
| Parity | None |
| Stop bits | 1 |
| Hardware flow control | No |

Boot Sequence

When you power on, a series of messages appears on the serial console. The message output is similar to the following:

```
Hardware:
UnitID: 003048724C52
Version: 4.5.12-B/1.2.5
Hostname: localhost
IP Address: 0.0.0.0
1) Show Configuration
2) Configure Ethernet
3) Configure Network
4) Configure DNS
5) Configure Passwords Menu
6) Configure Technical Support
7) Diagnostics Menu
8) Reboot
9) Shutdown
0) Quit
localhost>
```

Use the menu choices shown above to configure the administration port and establish network connectivity. The Show Configuration option allows you to verify the software version and administration interface configuration. Use the web-based Administration pages, as described in *Chapter 3, "Configuration and Management" in the Route Insight Manager Administration Guide*.

Most user prompts display the default values and accept the default if you press **ENTER**. Some menu items present more options depending on the choice you make at the first prompt. Each menu selection is described in more detail in the remainder of this chapter.

Show Configuration

This option displays the software version and network parameters of the administration interface. Auto Negotiate, Speed, and Duplex are the current interface states. After you reconfigure the interface, it may take a few seconds for this command to reflect the change. The UnitID field is required to upgrade the license. Table 12 on page 17 shows sample output.

Table 12: Show Configuration

| Menu Selection | localhost>1 |
|----------------|--|
| Output | <pre>Version: 5.0.06-B/2.0.0 Hardware: UnitID: 003048724C52 Ethernet Settings for Slot 0/Port 1 Auto Negotiate : Yes Speed : unknown Mbps Duplex : half Network Settings for Slot 0/Port 1 DHCP : Disabled IP Address : 10.123.234.56 Netmask : 255.255.255.0 Default Router : 10.123.232.1 Hostname : localhost DNS Primary DNS : 10.0.1.20 Technical Support Access : Enabled Callback : Enabled Administrative Interface: Slot 0/Port 1 —Hit <ENTER> to continue—</pre> |

Configure Ethernet

This menu selection sets the Ethernet parameters for the administration interface. Table 13 on page 17 shows sample output.

Table 13: Configure Ethernet

| Menu Selection | localhost>2 |
|--------------------------------|---|
| Output—Auto-negotiation | <pre>Ethernet settings for Slot 0/Port 1: (press <ENTER> to accept current setting) Auto Negotiate (y) [y/n]? y Are you sure you want to make this change [y/N]? y Please wait while changes are being applied.....</pre> |

Table 13: Configure Ethernet (*continued*)

| Menu Selection | localhost>2 |
|-------------------------------------|---|
| Output — No auto-negotiation | <pre> Ethernet settings for Slot 0/Port 1: (prompt <ENTER> to accept current setting) Auto Negotiate (y) [y/n]? n Speed (unknown) [10/100/1000]? 1000 Duplex (half) [h:half/f:full]? f Are you sure you want to make this change [y/N]? y Please wait while changes are being applied..... </pre> |

Configure Network

This menu selection enables or disables DHCP, and sets the IP address, Netmask, Default router, and Hostname.



NOTE: You must use a static IP address rather than DHCP.

Table 14 on page 18 shows sample output.

Table 14: Configure Network

| Menu Selection | localhost> |
|----------------|--|
| Output | <pre> Network settings for Slot 0/Port 1: (prompt <ENTER> to accept current setting) Use DHCP (n) [y/n]? n IP Address (0.0.0.0) : 10.123.234.56 Netmask (255.255.255.0) : 255.255.255.0 Default router (0.0.0.0) : 10.123.232.1 Hostname (localhost) : tex.lab.example.net Reset all other interfaces, aliases, and statically-configured routes [y/N]? n Are you sure you want to make this change [y/N]? y Please wait while changes are being applied.... </pre> |

Configure DNS

This menu selection sets the Domain Name Service (DNS) parameters when the DHCP server is disabled.

Table 15 on page 19 shows sample output.

Table 15: Configure DNS

| Menu Selection | localhost>4 |
|------------------------------|--|
| Output — DHCP Enabled | WARNING: DNS manual settings not supported while using DHCP. You must disable DHCP before changing DNS. (The configuration utility will return you to the main menu.) |
| Output— DHCP Disabled | DNS: (press <ENTER> to accept current setting) Primary DNS (0.0.0.0) : 10.0.1.20 Secondary DNS (0.0.0.0) : 10.128.1.20 Are you sure you want to make this change [y/N]? y Please wait while changes are being applied ... |

Configure Passwords Menu

This option displays a submenu to configure passwords for different purposes.

Table 16: Configure Passwords Menu

| Menu Selection | localhost>5 |
|----------------|--|
| Output | 1) Configure Console Password 2) Configure Master Access Password 3) Return to Main Menu |

The Configure Console Password option sets a password to protect access to the serial port console. If a console password is set, a password prompt is printed upon connecting to the serial console. By default, no password is set and so no prompt is printed to ask for a password. If a user disconnects from the serial console without quitting back to the password prompt, the console will remain logged in so the next user to connect will have access without needing to give the password again.

Table 17: Configure Console Password

| Menu Selection | localhost>1 |
|----------------|--|
| Output | <p>Enter new console password (no password): Re-enter new console password:</p> <p>If no password is entered and re-entered (the password is cleared), the following message is displayed:</p> <p>Console password cleared.</p> <p>If a new password is entered and re-entered, the following message is displayed:</p> <p>Console password updated.</p> <p>If the entered and re-entered passwords do not match, the following message is displayed:</p> <p>Passwords do not match, no change made.</p> |

If the appliance is part of a distributed configuration, the Management Console designated as the master will associate itself with client units through an HTTP POST. The Management Console authenticates that initial POST using the Master Access password. A default password is already set on all appliances as delivered, so it is not necessary to change this password. If you want to choose a different password, the same password must be set using this command on the master and on each of the clients. The password may be up to 250 characters long.

Table 18: Configure Master Access Password

| Menu Selection | localhost>2 |
|----------------|---|
| Output | <p>Enter new master access password (reset to default): Re-enter new master access password:</p> <p>If the entered and re-entered passwords match, the following message is displayed:</p> <p>Master access password updated.</p> <p>If the entered and re-entered passwords do not match, the following message is displayed:</p> <p>Passwords do not match, no change made.</p> |

Configure Technical Support Access

This option allows technical support to log through secure shell (SSH), if the appliance is on a publicly accessible IP address. If the appliance is connected to a network where direct remote access is not possible due to firewall restrictions, you can enable the “Technical support callback” feature. This feature is disabled by default and your explicit action is required to enable it. When you enable this feature, an SSH connection is initiated from the appliance to a dedicated and tightly secured server at Juniper. Firewall rules usually allow such outbound SSH connections. The appliance configures this connection in such a way that new login sessions can be tunneled from the server at Juniper through the SSH connection back to the appliance. As in the case of direct remote access, these login sessions use SSH and require a specially encrypted key.



NOTE: Enabling technical support callback enables technical support access. Disabling technical support access disables technical support callback.

Table 19 on page 21 shows sample output.

Table 19: Configure Technical Support Access

| Menu Selection | localhost>6 |
|--|---|
| Output—Technical Support disabled | Technical Support: (press <ENTER> to accept current setting) Enable Technical Support Access (e) [d:disable/e:enable]? d Are you sure you want to make this change [y/N]? y Disabling technical support access... Reloading sshd:[OK] Disabling technical support callback... |
| Output—Technical Support enabled | Technical Support: (press <ENTER> to accept current setting) Enable Technical Support Access (e) [d:disable/e:enable]? e Enable Technical Support Callback (d) [d:disable/e:enable]? d Are you sure you want to make this change [y/N]? y Enabling technical support access... Reloading sshd:[OK] Disabling technical support callback... |

Diagnostics Menu

This option displays the diagnostics menu.

Table 20: Diagnostics Menu

| Menu Selection | localhost>7 |
|----------------|--|
| Output | 1) Perform ping 2) Perform traceroute 3) Perform telnet 4) Perform tcpdump (on administrative interface) 5) Show Routing Table 6) Show Interface Statistics 7) Show Process Statistics 9) Return to Main Menu localhost> |

Table 21 on page 22 describes the diagnostic commands.

Table 21: Diagnostics Commands

| Command | User Input | Output |
|-----------------------|-------------------------|--|
| 1: Perform ping | Host name or IP address | Results of ping to the specified appliance. Also lists the available interfaces and takes a source interface selection. |
| 2: Perform traceroute | Host name or IP address | Trace of the route between the administrative interface port and the specified appliance. |
| 3: Perform telnet | Host name or IP address | Telnet connection attempt to the specified appliance. To forcibly disconnect an established telnet session, enter: CTRL-] close then press Enter . NOTE: The appliance does not accept incoming Telnet requests. |

Table 21: Diagnostics Commands (continued)

| Command | User Input | Output |
|------------------------------|--|---|
| 4: Perform tcpdump | Filter expression (optional) Number of packets to capture | Lists the available interfaces (physical and tunnels) with their system names, user-assigned names and addresses. This allows you to choose which system interface snoop, other than the administrative interface. Dump of network traffic on administrative interface. The system recognizes all filter expressions compatible with tcpdump 3.7.2 . Does not allow command line options (such as -w) in the filter expression. Accepts an optional filename parameter and writes to that filename in the /var/ftp directory. When output is to a file, the number of packets captured is limited to 1,000,000 to prevent filling the disk. |
| 5: Show Routing Table | None | Contents of the kernel IP routing table. |
| 6: Show Interface Statistics | None | Displays the output of ifconfig . |
| 7: Show Process Statistics | None | Displays the output of top . Several of the system processes (including kjournald) are filtered out to make the list more manageable. The output can be run once, N times, or until you enter Ctrl-C . |

Reboot

This menu selection reboots the appliance. The reboot command is also available on the web-based Administration Interface. Table 22 on page 23 shows sample output.

Table 22: Reboot Command

| Menu Selection | localhost>8 |
|----------------|--|
| Output | Are you sure you want to reboot [y/N]? y Rebooting ... |

Shutdown

Shutdown stops all internal tasks and powers down the appliance. Always use the shutdown command before switching off power. The shutdown command is also available on the web-based Administration page. Table 23 on page 24 shows sample output.

Table 23: Shutdown Command

| Menu Selection | localhost>9 |
|----------------|--|
| Output | Are you sure you want to shutdown [y/N]? y Shutting down ... |

List of Technical Publications

Table 24 on page 24 lists the software and hardware guides and release notes for Juniper Networks M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 25 on page 28 lists the books included in the *Network Operations Guide* series. Table 26 on page 29 lists the manuals and release notes supporting JUNOS Software for J-series and SRX-series platforms. All documents are available at <http://www.juniper.net/techpubs/>.

Table 27 on page 30 lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at <http://www.juniper.net/books>.

Table 24: Technical Documentation for Supported Routing Platforms

| Book | Description |
|---|---|
| JUNOS Software for Supported Routing Platforms | |
| <i>Access Privilege</i> | Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements. |
| <i>Broadband Subscriber Management Solutions</i> | Describes residential subscriber management and how you can deploy solutions that include multisubscriber IP address assignment, service provisioning, authentication, authorization, accounting, and dynamic request services in your network |
| <i>Class of Service</i> | Provides an overview of the class-of-service (CoS) functions of the JUNOS Software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm. |

Table 24: Technical Documentation for Supported Routing Platforms (continued)

| Book | Description |
|--|--|
| <i>CLI User Guide</i> | Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> . |
| <i>Feature Guide</i> | Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS Software. |
| <i>High Availability</i> | Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES). |
| <i>MPLS Applications</i> | Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols. |
| <i>Multicast Protocols</i> | Provides an overview of multicast concepts and describes how to configure multicast routing protocols. |
| <i>Multiplay Solutions</i> | Describes how you can deploy IPTV and voice over IP (VoIP) services in your network. |
| <i>MX-series Layer 2 Configuration Guide</i> | Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the <i>JUNOS Routing Protocols Configuration Guide</i> . |
| <i>MX-series Layer 2 Solutions Guide</i> | Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB). |
| <i>Network Interfaces</i> | Provides an overview of the network interface functions of the JUNOS Software and describes how to configure the network interfaces on the routing platform. |
| <i>Network Management</i> | Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options. |
| <i>Policy Framework</i> | Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options. |
| <i>Protected System Domain</i> | Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS Software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration. |

Table 24: Technical Documentation for Supported Routing Platforms (continued)

| Book | Description |
|--|---|
| <i>Routing Protocols</i> | Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols. |
| <i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i> | Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS Software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform. |
| <i>Services Interfaces</i> | Provides an overview of the services interfaces functions of the JUNOS Software and describes how to configure the services interfaces on the router. |
| <i>Software Installation and Upgrade Guide</i> | Describes the JUNOS Software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> . |
| <i>Subscriber Access</i> | Provides an overview of the subscriber access features of the JUNOS Software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods. |
| <i>System Basics</i> | Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network. |
| <i>VPNs</i> | Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples. |
| JUNOS References | |
| <i>Hierarchy and RFC Reference</i> | Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> . |
| <i>Interfaces Command Reference</i> | Describes the JUNOS Software operational mode commands you use to monitor and troubleshoot interfaces. |
| <i>Routing Protocols and Policies Command Reference</i> | Describes the JUNOS Software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters. |
| <i>System Basics and Services Command Reference</i> | Describes the JUNOS Software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring. |

Table 24: Technical Documentation for Supported Routing Platforms (continued)

| Book | Description |
|--|---|
| <i>System Log Messages Reference</i> | Describes how to access and interpret system log messages generated by JUNOS Software modules and provides a reference page for each message. |
| J-Web User Guide | |
| <i>J-Web Interface User Guide</i> | Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms. |
| JUNOS API and Scripting Documentation | |
| <i>JUNOScript API Guide</i> | Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms. |
| <i>JUNOS XML API Configuration Reference</i> | Provides reference pages for the configuration tag elements in the JUNOS XML API. |
| <i>JUNOS XML API Operational Reference</i> | Provides reference pages for the operational tag elements in the JUNOS XML API. |
| <i>NETCONF API Guide</i> | Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms. |
| <i>JUNOS Configuration and Diagnostic Automation Guide</i> | Describes how to use the commit script and self-diagnosis features of the JUNOS Software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies. |
| Hardware Documentation | |
| <i>Hardware Guide</i> | Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide. |
| <i>PIC Guide</i> | Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide. |
| <i>DPC Guide</i> | Describes the Dense Port Concentrators (DPCs) for all MX-series routers. |
| JUNOScope Documentation | |
| <i>JUNOScope Software User Guide</i> | Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations. |
| Advanced Insight Solutions (AIS) Documentation | |
| <i>Advanced Insight Solutions Guide</i> | Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices. |

Table 24: Technical Documentation for Supported Routing Platforms (continued)

| Book | Description |
|-------------------------------------|---|
| Release Notes | |
| <i>JUNOS Release Notes</i> | Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures. |
| <i>Hardware Release Notes</i> | Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes. |
| <i>JUNOScope Release Notes</i> | Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures. |
| <i>AIS Release Notes</i> | Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures. |
| <i>AIS AI-Scripts Release Notes</i> | Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back. |

Table 25: JUNOS Software Network Operations Guides

| Book | Description |
|---------------------------|--|
| <i>Baseline</i> | Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS Software, gathering basic system management information, verifying your network topology, and searching log messages. |
| <i>Interfaces</i> | Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms. |
| <i>MPLS</i> | Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network. |
| <i>MPLS Log Reference</i> | Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network. |
| <i>MPLS Fast Reroute</i> | Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing. |

Table 25: JUNOS Software Network Operations Guides (continued)

| Book | Description |
|-----------------|---|
| <i>Hardware</i> | Describes tasks for monitoring M-series and T-series routing platforms. |

To configure and operate a J-series Services Router or an SRX-series Services Gateway running JUNOS Software, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WX Integrated Services Module, you must also use WX documentation.

Table 26: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation

| Book | Description |
|---|---|
| J-series and SRX-series Platforms | |
| <i>JUNOS Software Interfaces and Routing Configuration Guide</i> | Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification. |
| <i>JUNOS Software Security Configuration Guide</i> | Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP). |
| <i>JUNOS Software Administration Guide</i> | Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems. |
| <i>JUNOS Software CLI Reference</i> | Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices. |
| <i>Network and Security Manager: Configuring J Series Services Routers and SRX Series Services Gateways Guide</i> | Explains how to configure, manage, and monitor J-series Services Routers and SRX-series services gateways through NSM. |
| <i>JUNOS Release Notes</i> | Summarize new features and known problems for a particular release of JUNOS Software, including JUNOS Software for J-series and SRX-series devices. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS Software. |
| J-series Only | |

Table 26: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation (continued)

| Book | Description |
|--|---|
| <i>JUNOS Software Design and Implementation Guide</i> | Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS Software. |
| <i>J Series Services Routers Quick Start</i> | Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity. |
| <i>JUNOS Software with Enhanced Services J-series Services Router Hardware Guide</i> | Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications. |
| <i>JUNOS Software Migration Guide</i> | Provides instructions for migrating an SSG device running ScreenOS software to JUNOS Software or upgrading a J-series device to a later version of the JUNOS Software. |
| <i>WXC Integrated Services Module Installation and Configuration Guide</i> | Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration. |

Table 27: Additional Books Available Through <http://www.juniper.net/books>

| Book | Description |
|---|--|
| <i>Interdomain Multicast Routing</i> | Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms. |
| <i>JUNOS Cookbook</i> | Provides detailed examples of common JUNOS Software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs. |
| <i>MPLS-Enabled Applications</i> | Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks. |
| <i>OSPF and IS-IS: Choosing an IGP for Large-Scale Networks</i> | Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks. |

Table 27: Additional Books Available Through <http://www.juniper.net/books> (continued)

| Book | Description |
|---|---|
| <i>Routing Policy and Protocols for Multivendor IP Networks</i> | Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers. |
| <i>The Complete IS-IS Protocol</i> | Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach. |

Revision History

26 August 2009—Beta Release. Document Revision 2

Copyright © 2009, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.